The Three C’s to Consider Before Deploying AI Technologies: Contracts, Compliance, and Culture

January 31, 2023

Authors

Chirag H. Patel , Myriah V. Jaworski

C #1: Contracts: Top Considerations for AI Vendor Management and Negotiating AI Contracts

In the age of innovation, many businesses are leveraging AI/ML technologies and automated decision-making tools to advance business objectives, save time and reduce costs. Automated solutions are increasingly used in candidate recruitment and hiring/promotion decisions, to deploy retail/digital marketing strategies, expedite claims processing and financial underwriting processes, or support healthcare decision making. The use cases and opportunities are nearly infinite.

And the law is starting to catch up. From New York City’s Local Law 144 (effective April 15, 2023) which requires bias audits of automated tool technologies used by New York City employers, to the EU’s Artificial Intelligence Act, regulators are taking a critical look at these technologies for their potential of producing biased or discriminatory outcomes. The US Equal Employment Opportunity Commission (EEOC) identified algorithmic integrity as a 2023 strategic enforcement initiative, and the National Institute of Technologies recently announced a risk management framework for the use of AI. Finalized rulemaking under the California Consumer Privacy Act (CCPA) is expected to address automated decision-making for advertising/profiling purposes, and other state privacy law proposals include similar provisions. Businesses are operating in a grey zone where the full scope of regulatory scrutiny over AI is quickly evolving and not fully known.

Before a business engages an AI-vendor or deploys an AI solution, there are three critical considerations: Contracts, Compliance, and Culture. This article is the first in a series and addresses the first C: Contracts.

AI Vendor Due Diligence & Scoping

When retaining any third-party vendor, a business should leverage its existing third-party vendor management/risk management procedures. This includes, but is not limited to vendor intake and due diligence, the use of information security questionnaires and risk profiles, and insurance coverage considerations. In the context of an AI vendor, special attention should be paid to the technical credentials and financial stability of the vendor, and whether and to what extent the vendor has Tech E&O coverage in place for defects with its solution.

A critical component of vendor management includes a scoping phase focused on the type of information shared with or to be processed by the vendor. For example, clarifying data sets and elements transmitted to the vendor is important to the business’s ability to instruct the vendor on its processing activities. If regulated personal information or confidential and proprietary business data will be transferred, a standalone data processing addendum should be executed that addresses vendor confidentiality, processing limitations, security standards, and deletion. State privacy laws, such as the California Consumer Privacy Act, as amended, and the newly effective Virginia Consumer Data Protection Act, require these vendor contracts to be in place.

For AI technologies, the scoping process should focus both on the type of data sets or materials that will be made available to the vendor in connection with the AI solution, and on reaching a consensus around the quality and accuracy of that data. This process is iterative, and vendor engagement is key. Further, the organization should have a clear understanding of how the solution works and the desirable outcomes, to assist in refining contractual provisions.

Last, many legislative proposals require businesses that process personal information as part of AI/ML tools or use AI/ML tools for automated decision making first conduct a privacy impact assessment before deploying such technology. While this onus is directly on the business that deploys the AI tool, the scoping process is an opportunity to obtain information required for the business to fully evaluate any privacy risks.

AI Contracts: Component Parts

Ordinarily, the provision of an AI Solution will be through an underlying vendor Master Services Agreement of Solutions Agreement, which will include standard contractual terms concerning the engagement, payment/fees, service level reps and warranties, liability, and termination provisions.

Most commonly, we see AI-specific terms set forth in an incorporated, but standalone, AI Addendum, especially where the AI Solution is provided as one part of a larger engagement (think a solution and services engagement). However, this is not required and businesses could certainly agree to bake the AI-specific terms directly into the primary agreement. The one potential benefit to having a standalone addendum is that – as we saw with cybersecurity addendums – it allows the parties to negotiate a different set of liability/indemnification provisions for AI-related liability, which may be different in scope from the standard term included in the master agreement.

Whether baked into the underlying agreement or subject to a separate addendum, the following provisions should be addressed in any AI-vendor contract:

- **Definitions:** The parties should define key AI terms to reflect the tool or technology, such as "algorithm," "AI solution," "data model" "input data" and "training data." This will require the parties to engage and answer practical questions – how, exactly, does this tool work, what is the training process like, what is the model deployed, and how does it evolve.
- **Use Rights:** Among other things, if the AI tool is based on an improving AI/ML model, a business should expect the vendor to grant the business rights to use the most recent and most trained iteration at all times.
- **Ownership:** Who owns the data? While Input Data likely belongs to the business, ownership rights in Trained Data may be shared. Alternatively, some businesses require strict confidentiality and ownership of all trained data and derivatives, and prohibit vendors from using such content in any way to develop training data or data models for third parties. Lastly, who owns the content at the time of termination and how that content should be returned to the business must be addressed. This term is negotiable and needs to be understood throughout the life of the business's use of the tool.
- **Representations and Warranties:** This is the meat of the AI contract. Here, a vendor will provide reps and warranties regarding the AI tool, including:
    - Free from material defects and substantially confirms with the desired outcome;
        - What is the desired outcome? Can an AI vendor really guarantee such an outcome?
        - Are Service Level Agreements (SLAs) appropriate for the tool at issue?
    - Data Accuracy: The parties must understand whether the business is warranting the accuracy and completeness of the Training Data, or not.
        - Some businesses choose to disavow and affirmatively not warrant the accuracy of this data, even if it means they will not get a similar representation from the vendor concerning the desired outcome.
- **Transparency & Audit Rights:** The vendor should be transparent in the use of the training data, input data, algorithms, and data models, and should agree to disclose the logic underlying the models to the business at its request. Oftentimes businesses also require the right to access and inspect (or potentially, audit) the vendor's use of the business data in an effort to verify the effectiveness of the vendor's solution, and its conformity with the contract and any applicable laws or regulations.
    - Bias Audits and Privacy Impact Assessments: In addition, depending on the AI tool and use case at issue, the parties may need to determine whether a bias audit of the tool is required, the frequency for such audit, who will conduct the audit, and the standards for same. New York Local Law 144

requires an annual bias audit of any automated decision-making tool used in the employment context by NYC employers, and other legislative proposals require bias audits and privacy impact assessments for the same.

- **Automated Final Decision Making:** Whether the tool will be used to make an automated final decision should be discussed and/or prohibited. Many businesses do not intend to use these tools for final automated decision making – i.e., without human monitoring, oversight, or ultimate approval. If that is the case, the parties should specify their intentions in the contract, and work to make sure the use of the tool for decision-making purposes is understood. If a vendor knows a business will use its technology to make automated decisions, the vendor can ask for the business to represent that it will do so in compliance with any existing laws or that it has a compliance program in place.
- **Liability and Indemnification:** It is difficult to fully evaluate the potential legal, reputational, and organizational risks of deploying an AI tool, in large part because AI regulation is just starting to be enacted. Thus, the parties should work collaboratively together to understand who they will share, or not, potential direct and third-party liability, including liability for consumer claims and regulatory enforcement in the event of an allegation of bias/discrimination. Here, too, insurance coverage requirements should be considered.

Negotiating an AI contract is an opportunity for the parties to dig deep into the technology, data, and use case. Retaining experienced legal counsel is critical, especially to assist in the negotiation of AI contracts for tools and technologies which can provide your business with many efficiency gains, but also pose uncertain legal and reputational risks.

Stay tuned for follow-up articles in this series evaluating the remaining Cs of Deploying AI Technologies: Compliance and Culture.

For the second article in this series, on Compliance, click here.

The views and opinions expressed in the article represent the view of the authors and not necessarily the official view of Clark Hill PLC. Nothing in this article constitutes professional legal advice nor is it intended to be a substitute for professional legal advice.

Related Practice Areas

Cybersecurity, Data Protection & Privacy

Related

Legal Updates

HHS Issues Notice of Proposed Rulemaking on Reproductive Health Care Privacy

Legal Updates

The Intersection Between Marijuana and the 2nd Amendment: What Gun Owners Need to Know

Marijuana use has become increasingly common in the United States, with many states legalizing its use for medical or recreational purposes. However, US federal law still classifies marijuana as a Schedule I drug, which means it is illegal under federal law. This creates a confusing legal landscape that can impact the rights of citizens, particularly when it comes to the U.S. Constitutional Second Amendment right to bear arms. In this article, we will explore how U.S. marijuana laws affect citizens' rights to bear arms and what this means for those who use marijuana.

Legal Updates

Your Employees Are Using ChatGPT and Other LLMs: Risks and Legal Implications of ChatGPT in the Workplace

The Clark Hill approach is equally pragmatic and growth-minded, which is why we understand our clients’ toughest business challenges. Our multidisciplinary, global team of advisors focuses on smart legal solutions, delivered simply.

Contact Us

Policies & Disclaimers

Client Log-in

Payments

Employee Resources